N/MCI Contract N00024-00-D-6000
Awarded 6 October 2000

Attachment 8
Information Assurance
Smart Card Specifications

I. Smart Cards

a. General Information:
The smart card is a portion of the Department of the Navy's Information Assurance vision. Initially, smart cards will be utilized for sensitive, but unclassified networks only. The below sections (b to e) discuss the smart card's intended functionality, specifications, and its interaction with the DON's client workstations and devices.

b. Intended Functionality:
The smart card specified below is intended to support cryptographic functions for a system that utilizes two sets of key pairs and certificates (Authentication and Encryption).

The authentication keys will be used for digital signing and secure authentication. The key pairs will be generated on the card. The public key will be securely sent to the CA where the CA creates a X.509 v3 digital certificate from the public key and signs it with the CA's private key. The X.509 v3 certificate is sent to the card to be securely stored.

The Encryption keys will be used for encryption functions. These key pairs will be generated in software. The public key will be securely sent to the CA where the CA creates a X.509 v3 digital certificate from the public key and signs it with the CA's private key. Conversely, the private key in software will be wrapped, encrypted, and securely sent to the CA. The CA will escrow the private key. Once the CA has securely received the card's private key, it will send the X.509 v3 digital certificate to the card for secure storage. All keying material created in software will be securely deleted from memory.

c. Card Specifications:
The leveraging of industry standards and specifications for Commercial Off The Shelf (COTS) products is the foundation of the smart card technical specifications. They are as follows:

Standards:

- ISO 7816, 1-4
- Asychronous (T=1, T=0)
- EMV
- Java Card 2.1 or Windows Powered Smart Card v 1.0
- Built into the ROM or EEPROM should be the ability to securely store/load on-card applications or applets such that any application or applet dynamically entered into the card platform must be identified by the card as an authorized set of code
- The card will contain a defined PKCS#15 file structure for the cryptographic functions of the card.
- FIPS 140-1, Level 2 certified (or in the certification process)

Micro-controller and Processing

- Minimum: 16K micro-controller (with 16K of available EEPROM)
- Minimum: 8-bit processor
- Crypto co-processor with a pseudo-random number generator.

Cryptography

- Triple DES
- RSA
- Minimum 1024 bit RSA key length
- SHA-1
- MD5 (optionally)
- On card key generation-RSA

Card-Based Authentication

- Minimally: the cryptographic functions will require a Personal Identification Number (PIN), password, or biometric authentication.
- Other function of the card may require a PIN, password, or biometric as required by the application and operational environment.

Card Physical Characteristics

- Card composition will be 30 mm PVC plastic
- Contain a top-mounted standard American Bankers Association (ABA) 3 Track magnetic stripe on the back.
- Magnetic stripe to be high coercivity (4000 Oersted).
- The remaining portion of the card will be blank white card stock.

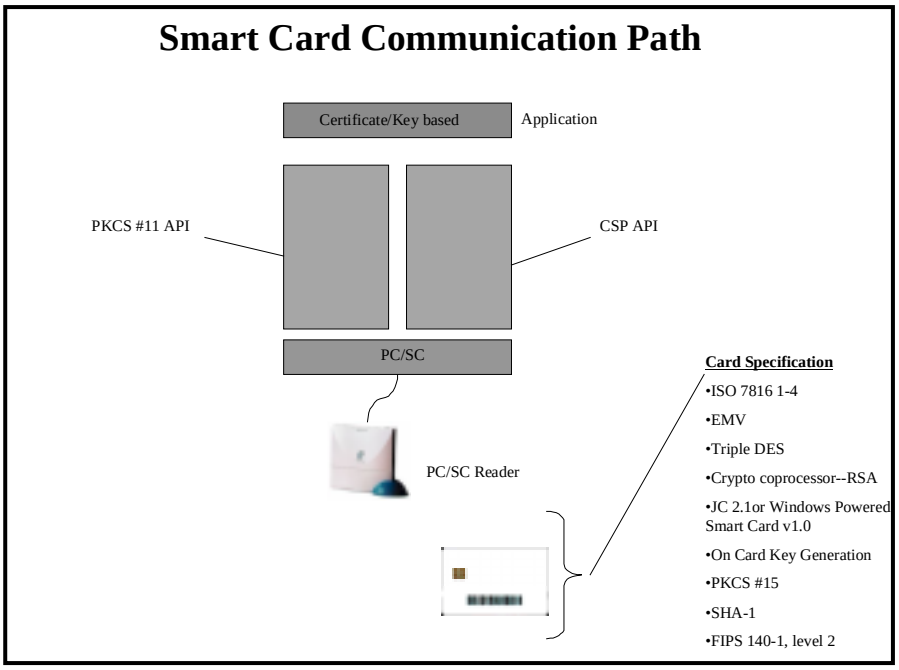
d. Optional Functionality:

Contactless Functionality

Some DON personnel may have a need to access building, ships, or locations via the contactless interface on a smart card. Smart card can be a key tool in enabling access control systems via the different of technologies that may be on the smart card medium (ie magnetic stripe, contactless, visual identification, and bar code). A predetermined number of smart cards will contain both the contact features listed below and contactless.

e. Smart Card Cryptographic APIs:

The contractor shall provide cryptographic middleware. The below diagram illustrates these communication protocols.



II. Smart Card Readers:

Smart card readers will be needed to interact with the smart card client tokens in a Microsoft Windows 95, 98, NT 4.0 or higher; UNIX; LINIX; and JavaOS environments. Depending on the client operating system, smart card readers should minimally be PC/SC (WHQL logoed) certified or Open Card Framework compliant.

The DON is open to examining additional interfaces and/or alternatives. Venders are encouraged to present, as long as the vendors minimally address the below items.

a. <u>Desktop workstations:</u>

Reader Embedded in Workstation*:*

<u>General Specification:</u>

- 1 L.E.D with dual displaying power-on and read/write
- T=1 and T=0 protocol support
- Frequency-1-5 MHz
- Software updates for new smart card protocols and APIs should be provided

<u>Protocol management/ communication:</u>

- Support data exchange 9600 to 115, 200 or greater bps (smart card to reader)

<u>Power:</u>

- Powered via PS/2 port (or optional DIN5 connector)
- 3V and 5V smart card compatible
- Compliant with IS0 7816 and EMV (5V, 60mA)

Physical Characteristics
- Minimally 100,000 insertion cycles
- ISO chip location

Optional Features:
- Short circuit detection to protect smart card and reader

9 pin RS-232 Serial Interface:

General Specification:
- 1 L.E.D with dual displaying power-on and read/write
- T=1 and T=0 protocol support
- Frequency-1-5 MHz
- Software updates for new smart card protocols and APIs should be provided
- At least 1-2 meter cable

Protocol management/ communication:
- Support data exchange 9600 to 115, 200 or greater bps (smart card to reader)

Power:
- Powered via PS/2 port (or optional DIN5 connector)
- 3V and 5V smart card compatible
- Power supply compliant with IS0 7816 and EMV (5V, 60mA)

Physical Characteristics
- Minimally 100,000 insertion cycles
- ISO chip location
- Enclosure or casing should contain an additional base for vertical positioning or sit vertically.

Optional Features:
- Short circuit detection to protect smart card and reader

USB 1.0 Port Interface:

General Specification:
- 1 L.E.D with dual displaying power-on and read/write
- T=1 and T=0 protocol support
- Frequency-1-5 MHz
- Software updates for new smart card protocols and APIs should be provided
- At least 1-2 meter cable

Protocol management/ communication:
- Support data exchange 9600 to 115, 200 or greater bps (smart card to reader)

Power:
- USB 1.0
- 3V and 5V smart card compatible
- Power supply compliant with IS0 7816 and EMV (5V, 60mA)

Physical Characteristics
- Minimally 100,000 insertion cycles
- ISO chip location
- Enclosure or casing should contain an additional base for vertical positioning or sit vertically.

Optional Features:
- Short circuit detection to protect smart card and reader

b. Portable Laptop workstations:

PCMCIA Interface:

General Specification:
- PCMCIA Type II Interface
- T=1 and T=0 protocol support
- Frequency-1-5 MHz
- Software updates for new smart card protocols and APIs should be provided

Protocol management/ communication:
- Support data exchange 9600 to 115, 200 or greater bps (smart card to reader)

Power:
- 3V and 5V smart card compatible
- Power supply compliant with IS0 7816 and EMV (5V, 60mA)

Physical Characteristics
- Up to 100,000 insertion cycles
- ISO chip location

Optional Features:
- Short circuit detection to protect smart card and reader

9 pin RS-232 Serial Interface:

General Specification:
- 1 L.E.D with dual displaying power-on and read/write
- T=1 and T=0 protocol support
- Frequency-1-5 MHz
- Software updates for new smart card protocols and APIs should be provided
- At least 1-2 meter cable

Protocol management/ communication:

- Support data exchange 9600 to 115, 200 or greater bps (smart card to reader)

Power:

- Powered via PS/2 port (or optional DIN5 connector)
- 3V and 5V smart card compatible
- Power supply compliant with IS0 7816 and EMV (5V, 60mA)

Physical Characteristics

- Minimally 100,000 insertion cycles
- ISO chip location
- Enclosure or casing should contain an additional base for vertical positioning or sit vertically.

Optional Features:

- Short circuit detection to protect smart card and reader

USB 1.0 Port Interface:

General Specification:

- 1 L.E.D with dual displaying power-on and read/write
- T=1 and T=0 protocol support
- Frequency-1-5 MHz
- Software updates for new smart card protocols and APIs should be provided
- At least 1-2 meter cable

Protocol management/ communication:

- Support data exchange 9600 to 115, 200 or greater bps (smart card to reader)

Power:

- USB 1.0
- 3V and 5V smart card compatible
- Power supply compliant with IS0 7816 and EMV (5V, 60mA)

Physical Characteristics

- Minimally 100,000 insertion cycles
- ISO chip location
- Enclosure or casing should contain an additional base for vertical positioning or sit vertically.

Optional Features:

- Short circuit detection to protect smart card and reader
-

c. Other Portable Wireless Devices (ie Personal Digital Assistant (PDA), cell phones, and/or others)

It is anticipated that a smart card interface will be necessary for other portable wireless devices. The vendor should discuss the type of interface (s) that could be provided as either integrated or peripherally attached.